

DIGIPASS
software

DIGIPASS CertiID

Getting Started

Disclaimer of Warranties and Limitations of Liabilities

The Product is provided on an 'as is' basis, without any other warranties, or conditions, express or implied, including but not limited to warranties of merchantable quality, merchantability of fitness for a particular purpose, or those arising by law, statute, usage of trade or course of dealing. The entire risk as to the results and performance of the product is assumed by you. Neither we nor our dealers or suppliers shall have any liability to you or any other person or entity for any indirect, incidental, special or consequential damages whatsoever, including but not limited to loss of revenue or profit, lost or damaged data of other commercial or economic loss, even if we have been advised of the possibility of such damages or they are foreseeable; or for claims by a third party. Our maximum aggregate liability to you, and that of our dealers and suppliers shall not exceed the amount paid by you for the Product. The limitations in this section shall apply whether or not the alleged breach or default is a breach of a fundamental condition or term, or a fundamental breach. Some states/countries do not allow the exclusion or limitation or liability for consequential or incidental damages so the above limitation may not apply to you.

Copyright

© 2008, 2009 VASCO Data Security. All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of VASCO Data Security Inc.

Trademarks

VASCO, VACMAN, IDENTIKEY, aXsGUARD, DIGIPASS and the Vasco 'V' logo are either registered or unregistered trademarks of VASCO Data Security, Inc. and/or VASCO Data Security International GmbH in the U.S. and other countries.

Version: 2009-06-12

Table of Contents

1	Introduction	7
1.1	About this Manual	8
1.1.1	How to Use this Manual.....	8
1.1.2	Document Conventions	8
1.1.3	Providing Feedback.....	9
2	Requesting and Enrolling Certificates	10
2.1	Enrolling Certificates from a Microsoft Certification Authority (CA) using the CA Web interface	11
2.1.1	Before you begin.....	11
2.1.2	Enrolling a certificate from a Microsoft Certification Authority (CA).....	12
2.1.3	Additional considerations.....	14
2.1.4	Additional references	14
2.2	Enrolling Certificates from a Microsoft Certification Authority (CA) using Microsoft Management Console (MMC) 15	
2.2.1	Before you begin.....	15
2.2.2	Enrolling a certificate from a Microsoft CA using MMC	15
2.2.3	Additional considerations.....	19
2.3	Enrolling Certificates from Microsoft Certificate Lifecycle Manager (CLM)	20
2.3.1	Before you begin.....	20
2.3.2	Enrolling a certificate from Microsoft Certificate Lifecycle Manager (CLM).....	20
2.3.3	Additional considerations.....	23
2.3.4	Additional references	23
2.4	Enrolling Certificates from an Entrust Certification Authority (CA)	24
2.4.1	Before you begin.....	24
2.4.2	Enrolling a certificate from an Entrust Certification Authority (CA)	24
2.4.3	Additional considerations.....	29
2.4.4	Additional references	29
3	Signing and Encrypting E-mails	30
3.1	Signing and Encrypting E-mails with Microsoft Outlook 2003	31
3.1.1	Before you begin.....	31
3.1.2	Signing and Encrypting an E-mail with Microsoft Outlook 2003.....	33
3.1.3	Additional considerations.....	35
3.1.4	Additional references	35
3.2	Signing and Encrypting E-mails with Mozilla Thunderbird 2.x.....	36
3.2.1	Before you begin.....	36
3.2.2	Signing and Encrypting an E-mail with Mozilla Thunderbird 2.x.....	39
3.2.3	Additional considerations.....	40
3.2.4	Additional references	40

4	Signing Documents	41
4.1	Signing Documents with Adobe Acrobat 8.x	42
4.1.1	Before you begin.....	42
4.1.2	Signing a document with Adobe Acrobat 8.x.....	42
4.1.3	Additional considerations.....	43
4.1.4	Additional references	43
5	Encrypting Documents.....	44
5.1	Encrypting Documents with Adobe Acrobat 8.x.....	45
5.1.1	Before you begin.....	45
5.1.2	Encrypting a document with Adobe Acrobat 8.x	45
5.1.3	Additional references	45
6	Encrypting Files and Folders.....	46
6.1	Encrypting and Decrypting Files and Folders via Encrypting File System (EFS)	47
6.1.1	Before you begin.....	47
6.1.2	Encrypting a file or a folder using Encrypting File System (EFS)	48
6.1.3	Decrypting a file or a folder using Encrypting File System (EFS).....	49
6.1.4	Additional considerations.....	49
6.1.5	Additional references	50
6.2	Recovering Data for Encrypting File System (EFS)	51
6.2.1	Before you begin.....	51
6.2.2	Recovering data for Encrypting File System (EFS) using file recovery	52
6.2.3	Recovering data for Encrypting File System (EFS) using key recovery.....	53
6.2.4	Additional references	53
7	Certificate-based Authentication	54
7.1	Authenticating to Microsoft Windows XP/2000	55
7.1.1	Before you begin.....	55
7.1.2	Authenticating to Microsoft Windows XP/2000	55
7.1.3	Additional considerations.....	55
7.1.4	Additional references	56
7.2	Authenticating to Microsoft Windows Vista.....	57
7.2.1	Before you begin.....	57
7.2.2	Authenticating to Microsoft Windows Vista	57
7.2.3	Additional considerations.....	58
7.2.4	Additional references	58

Illustration Index

Figure 1: Enrolling a Certificate from a Microsoft CA (1)	12
Figure 2: Enrolling a Certificate from a Microsoft CA (2)	13
Figure 3: Enrolling a Certificate from Microsoft Certificate Lifecycle Manager via MMC (1).....	16
Figure 4: Enrolling a Certificate from Microsoft Certificate Lifecycle Manager via MMC (2).....	17
Figure 5: Enrolling a Certificate from Microsoft Certificate Lifecycle Manager via MMC (3).....	18
Figure 6: Enrolling a Certificate from Microsoft Certificate Lifecycle Manager via MMC (4).....	19
Figure 7: Enrolling a Certificate from Microsoft Certificate Lifecycle Manager (1).....	21
Figure 8: Enrolling a Certificate from Microsoft Certificate Lifecycle Manager (2).....	22
Figure 9: Enrolling a Certificate from Microsoft Certificate Lifecycle Manager (3).....	23
Figure 10: Enrolling a Certificate from an Entrust CA using Entrust ESP (1).....	25
Figure 11: Enrolling a Certificate from an Entrust CA using Entrust ESP (2).....	25
Figure 12: Enrolling a Certificate from an Entrust CA using Entrust ESP (3).....	26
Figure 13: Enrolling a Certificate from an Entrust CA using Entrust Desktop Solutions (1)	27
Figure 14: Enrolling a Certificate from an Entrust CA using Entrust Desktop Solutions (2)	27
Figure 15: Enrolling a Certificate from an Entrust CA using Entrust Desktop Solutions (3)	28
Figure 16: Enrolling a Certificate from an Entrust CA using Entrust Desktop Solutions (4)	28
Figure 17: Enrolling a Certificate from an Entrust CA using Entrust Desktop Solutions (5)	29
Figure 18: Configuring E-mail security in Microsoft Outlook 2003 (1)	32
Figure 19: Configuring E-mail Security in Microsoft Outlook 2003 (2).....	33
Figure 20: Signing and Encrypting an E-mail with Microsoft Outlook 2003	34
Figure 21: Registering DP CertiID PKCS#11 Library with Mozilla Thunderbird 2.x (1).....	37
Figure 22: Registering DP CertiID PKCS#11 Library with Mozilla Thunderbird 2.x (2).....	37

Figure 23: Registering DP CertiID PKCS#11 Library with Mozilla Thunderbird 2.x (3).....	38
Figure 24: Configuring E-mail Security in Mozilla Thunderbird 2.x.....	38
Figure 25: Signing and Encrypting an E-mail with Mozilla Thunderbird 2.x.....	39
Figure 26: Signing a Document with Adobe Acrobat 8.x.....	43
Figure 27: Authenticating to Microsoft Windows XP/2000 using a Certificate	55
Figure 28: Authenticating to Microsoft Windows Vista using a Certificate	57

1 Introduction

Welcome to the DIGIPASS CertiID Getting Started. This document provides you the information you will need to use DIGIPASS CertiID with common third-party applications.

This manual provides information about how to use DIGIPASS CertiID to:

- enroll certificates from a Microsoft Certification Authority (CA)
- enroll certificates from Microsoft Certificate Lifecycle Manager (CLM)
- enroll certificates from an Entrust Certification Authority (CA)
- sign and encrypt E-mails with Microsoft Outlook 2003
- sign and encrypt E-mails with Mozilla Thunderbird 2.x
- sign and encrypt documents with Adobe Acrobat 8.x
- encrypt files and folders with Encrypting File System (EFS)
- authenticate to Microsoft Windows Vista/XP/2000

This manual does **not** provide:

- detailed instructions about preparing and installing DIGIPASS CertiID (refer to DIGIPASS CertiID Installation Guide)
- a detailed introduction to DIGIPASS CertiID, its features, and components (refer to DIGIPASS CertiID User Manual)
- detailed instructions about using and configuring DIGIPASS CertiID applications (refer to DIGIPASS CertiID User Manual)

1.1 About this Manual

1.1.1 How to Use this Manual

You can use this manual in different ways, depending on your skill and knowledge level. You can read it from the beginning to the end (highly recommended for novice users), you can browse through the chapter abstracts and read specifically the chapters relevant to your needs, or you can search by key words in the index, if you need to find certain references quickly.

If you need to...	Refer to
...enroll a certificate from a Microsoft Certification Authority (CA) to use with DIGIPASS CertiID -OR- ...enroll a certificate from a Microsoft Certificate Lifecycle Manager (CLM) to use with DIGIPASS CertiID -OR- ...enroll a certificate from an Entrust Certification Authority (CA) to use with DIGIPASS CertiID	Chapter " 2 Requesting and Enrolling Certificates "
...use DIGIPASS CertiID to sign or encrypt E-mails with Microsoft Outlook 2003	Section " 3.1 Signing and Encrypting E-mails with Microsoft Outlook 2003 "
...use DIGIPASS CertiID to sign or encrypt E-mails with Mozilla Thunderbird 2.x	Section " 3.2 Signing and Encrypting E-mails with Mozilla Thunderbird 2.x "
...use DIGIPASS CertiID to sign and verify PDF documents with Adobe Acrobat 8.x	Section " 4.1 Signing Documents with Adobe Acrobat 8.x "
...use DIGIPASS CertiID to encrypt PDF documents with Adobe Acrobat 8.x	Section " 5.1 Encrypting Documents with Adobe Acrobat 8.x "
...use DIGIPASS CertiID to encrypt PDF documents with Adobe Acrobat 8.x	Section " 5.1 Encrypting Documents with Adobe Acrobat 8.x "
...use DIGIPASS CertiID to encrypt files and folders with Encrypting File System (EFS)	Section " 6.1 Encrypting and Decrypting Files and Folders via Encrypting File System (EFS) "
...use DIGIPASS CertiID for certificate-based authentication to Microsoft Windows Vista	Section " 7.2 Authenticating to Microsoft Windows Vista "

1.1.2 Document Conventions

The following typographic style conventions are used throughout this document.

Typography	Meaning
Boldface	Names of user interface widgets, e.g. the OK button
Blue	Values for options; placeholders for information or parameters that you provide, e.g. select Server name in the list box.
UPPERCASE	Keyboard keys, e.g. CTRL for the Control key
Monospace	Windows Registry Keys; commands you are supposed to type in or are displayed in a command prompt shell, including directories and filenames; API functions and source code examples

Typography	Meaning
<u>blue, underlined</u>	Internet links

The following visual hint colour schemes are used throughout this document.

TIP

Tips contain supplementary information that is not essential to the completion of the task at hand, including explanations of possible results or alternative methods.

NOTE

Notes contain important supplementary information.

CAUTION

Cautions contain warnings about possible data loss, breaches of security, or other more serious problems.

1.1.3 Providing Feedback

Every effort has been made to ensure the accuracy and usefulness of this manual. However, as the reader of this documentation, *you* are our most important critic and commentator. We appreciate your judgment and would like you to write us your opinions, suggestions, critics, questions, and ideas. Please send your commentary to: documentation@vasco.com.

To recognize the particular document you are referring to, please include the following information in your subject header: DPC-GS-3.1.0en-12062009

Please note that product support is not offered through the above mail address.

2 Requesting and Enrolling Certificates

This chapter gives an overview of how to request and enroll certificates from different certification authorities (CA) to use with your token and DIGIPASS CertiID.

It covers the following topics:

- Enrolling Certificates from a Microsoft Certification Authority (CA) using the CA Web interface
- Enrolling Certificates from a Microsoft Certification Authority (CA) using Microsoft Management Console (MMC)
- Enrolling Certificates from Microsoft Certificate Lifecycle Manager (CLM)
- Enrolling Certificates from an Entrust Certification Authority (CA)

2.1 Enrolling Certificates from a Microsoft Certification Authority (CA) using the CA Web interface

2.1.1 Before you begin

To request and enroll a certificate from a Microsoft CA using the Web interface you need:

- access to the Web interface of the respective CA
- a certificate template defined on the CA
- Microsoft Internet Explorer
- an initialized token
- **VASCO CertiID Smart Card Crypto Provider** installed

-OR-

VASCO Card Module installed and registered as default cryptographic provider

2.1.2 Enrolling a certificate from a Microsoft Certification Authority (CA)

➤ To enroll a certificate from a Microsoft CA using the CA Web interface

1. Start Microsoft Internet Explorer and go to the Web site of your CA, e.g. <http://myCA.com/certsrv/>.

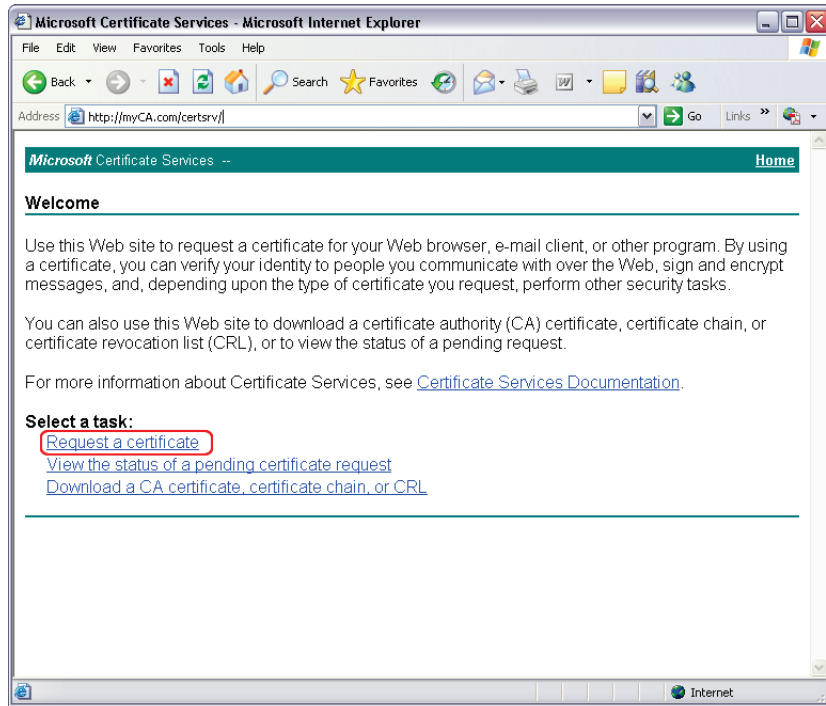


Figure 1: Enrolling a Certificate from a Microsoft CA (1)

2. If required, enter your user credentials to log on to the CA Web site.
3. Click **Request a certificate**.
4. Click **Create and submit a request to this CA**.

If you visit the site the first time, an ActiveX control is downloaded and installed.

- Configure your certificate request in the **Advanced Certificate Request Form**:

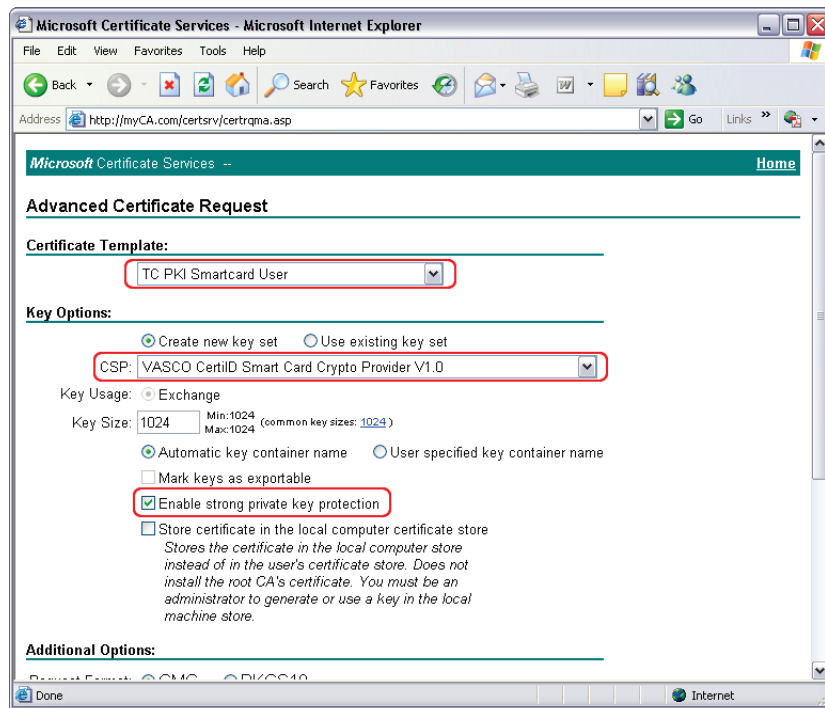


Figure 2: Enrolling a Certificate from a Microsoft CA (2)

- Select a certificate template in the **Certificate Template** list.
- Select **Create new key set**.

TIP

You can select a key pair already existing on the token (e.g. if you have deleted the associated certificate) to create and associate a certificate to it. To do so, select **Use existing key set**. Then type the GUID of the respective key container on the token in **Container Name** box.

- Select the correct cryptographic service provider in the **CSP** list, i.e.
 - select **VASCO CertiID Smart Card Crypto Provider**, if you want to use **VASCO CertiID Smart Card Crypto Provider**
 - select **Microsoft Base Smart Card Crypto Provider**, if you want to use **VASCO Card Module**
- Select the key size for the key pair.

The theoretically supported key size is between 512 to 2048 bytes. The effectively available key size depends on the capabilities of the particular token and reader.

- Select **Enable strong private key protection** to protect the secret key of the new certificate with the default PIN.

11. Click **Submit** to send the request to the CA.
12. If required, confirm the request by clicking **Yes**.
13. If not already done, insert your token.
14. If you have more than one token connected, select the token to enroll the certificate on in the **Select Token Dialog** and click **Next**.
15. If required, enter the default PIN for your token.
16. Click **Install the certificate now** to store the certificate on the token and to add it to the local certificate store.

2.1.3 Additional considerations

- The new private key associated with the requested certificate is protected by the default PIN, if one is available on the token. You can change this via **DP CertiID Management Application**.
- Usually you are required to supersede and configure certificate templates to enroll from existing certificate templates pre-configured on the Microsoft CA.
- Certificate templates for Microsoft CAs should require a minimum key length of 1024 bits, if you are going to enroll to tokens based on STARCOS.

2.1.4 Additional references

- [Enrolling Certificates from an Entrust Certification Authority \(CA\)](#)
- [Enrolling Certificates from Microsoft Certificate Lifecycle Manager \(CLM\)](#)

2.2 Enrolling Certificates from a Microsoft Certification Authority (CA) using Microsoft Management Console (MMC)

2.2.1 Before you begin

To request and enroll a certificate from a Microsoft CA using Microsoft Management Console you need:

- network access to the respective CA
- a certificate template defined on the CA
- Microsoft Management Console (MMC)
- an initialized token
- **VASCO CertiID Smart Card Crypto Provider** installed

-OR-

VASCO Card Module installed and registered as default cryptographic provider

2.2.2 Enrolling a certificate from a Microsoft CA using MMC

- To enroll a certificate from a Microsoft CA via Microsoft Management Console (MMC)
1. Start Microsoft Management Console by typing `mmc` in a command line prompt.
 2. If the Console Root tree does not contain the **Certificates** snap-in, add the snap-in by doing the following:
 - (a) Select **File > Add / Remove Snap-in**.
 - (b) Highlight the **Certificates** snap-in in the **Available snap-ins** list and click **Add**.
 - (c) Select **My user account** and click **Finish**.
 - (d) Click **OK** to return to Microsoft Management Console.

3. Select **Certificates – Current User** in the Console Root tree.

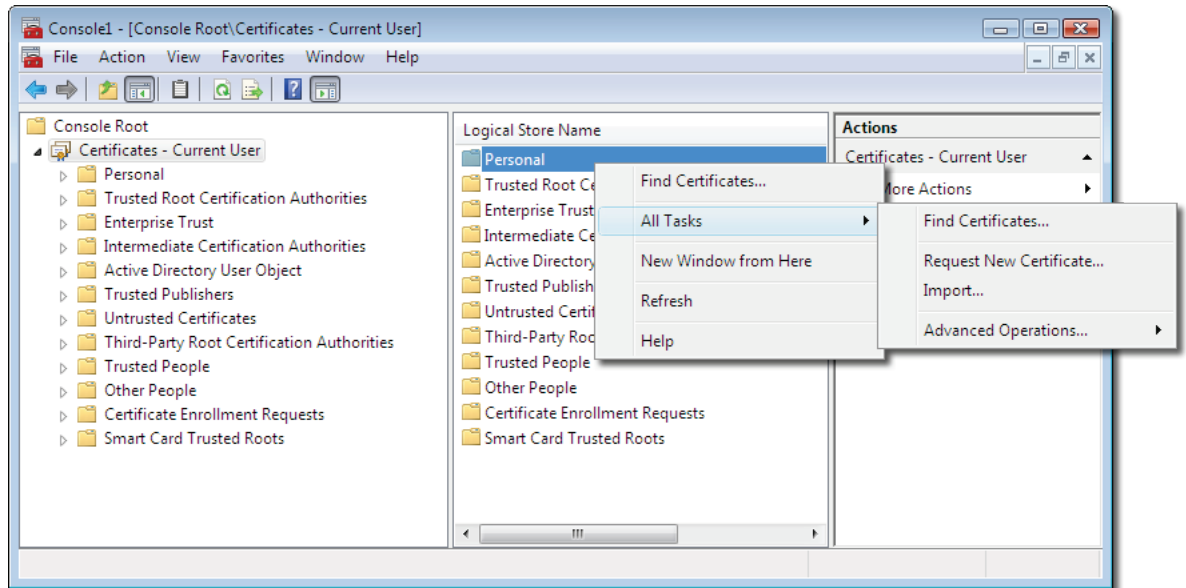


Figure 3: Enrolling a Certificate from Microsoft Certificate Lifecycle Manager via MMC (1)

4. In **Logical Store Name** select **Personal > All Tasks > Request New Certificate**.

The **Certificate Enrollment Wizard** appears.

5. Click **Next**.

6. Check the desired certificate type.

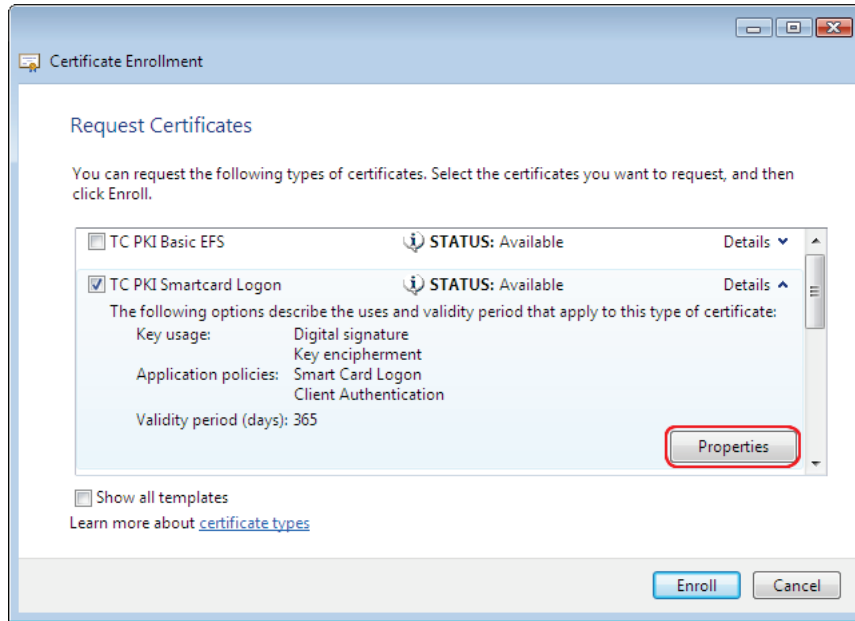


Figure 4: Enrolling a Certificate from Microsoft Certificate Lifecycle Manager via MMC (2)

7. Expand the certificate type item via **Details** and click **Properties**.

The **Certificate Properties Dialog** appears.

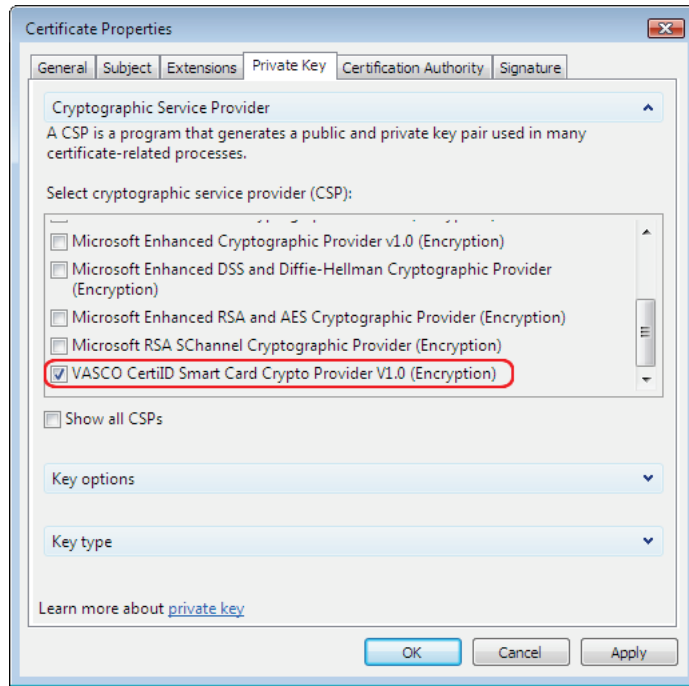


Figure 5: Enrolling a Certificate from Microsoft Certificate Lifecycle Manager via MMC (3)

- (a) Switch to the **Private Key** tab.
- (b) Expand the **Cryptographic Service Provider** list.
- (c) Select **VASCO CertID Smart Card Crypto Provider** and deselect any other CSP in the list, if you want to use **VASCO CertID Smart Card Crypto Provider**.

-OR-

Select **Microsoft Base Smart Card Crypto Provider** and deselect any other CSP in the list, if you want to use **VASCO Card Module**.

- (d) Expand the **Key options** list.
- (e) Clear **Make private key exportable**.
- (f) Click **OK** to return to the **Certificate Enrollment Wizard**.

8. Click **Enroll**.
9. If required, insert your token.

10. If required, enter your PIN.

The certificate request is created and submitted to the certification authority.

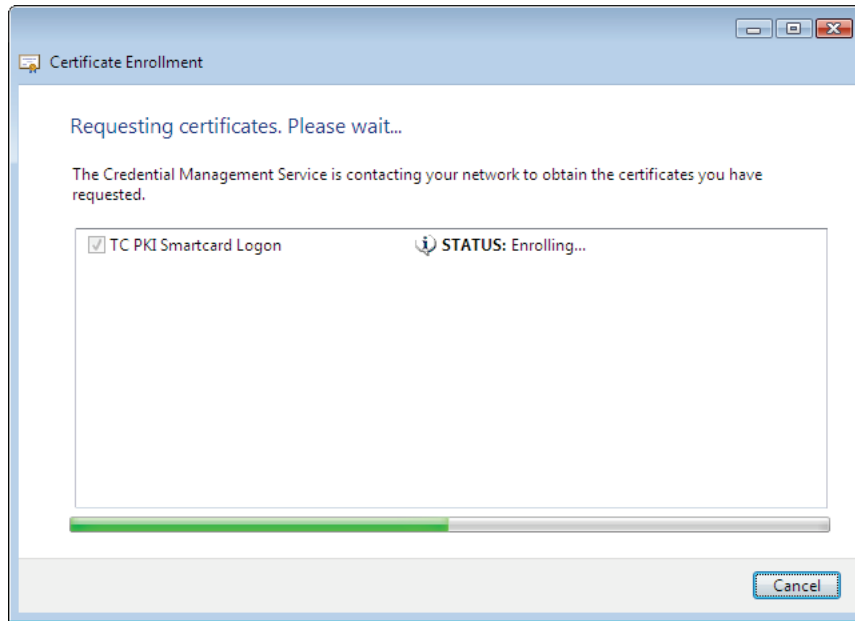


Figure 6: Enrolling a Certificate from Microsoft Certificate Lifecycle Manager via MMC (4)

11. Click **Finish**.

2.2.3 Additional considerations

- The system administrator may restrict access to certain snap-ins by Local Policies or Group Policies. If the **Certificate** snap-in is not available, you may not have privileges to use it.
- Usually you are required to supersede and configure certificate templates to enroll from existing certificate templates pre-configured on the Microsoft CA.

2.3 Enrolling Certificates from Microsoft Certificate Lifecycle Manager (CLM)

2.3.1 Before you begin

To request and enroll a certificate from a Microsoft Certificate Lifecycle Manager (CLM) you need:

- access to the Web interface of the respective CLM server (if using the CLM Web interface)
- to specify the CLM Web site in the [Trusted Sites](#) zone in the Web browser settings (if using the CLM Web interface)
- a profile template defined on the CLM
- privileges to access the profile template
- the user defined within Microsoft Active Directory or Microsoft CLM
- Microsoft Internet Explorer installed
- Microsoft Certificate Lifecycle Manager Client installed
- **VASCO Card Module** installed
- an initialized token with PIN and administrator key; the administrator key must match the configured profile template

2.3.2 Enrolling a certificate from Microsoft Certificate Lifecycle Manager (CLM)

You can enroll a certificate from Microsoft CLM via the CLM Web interface.

➤ **To enroll a certificate from Microsoft CLM using the CLM Web interface**

1. Insert your token.
2. Start Microsoft Internet Explorer and go to the Web site of your CLM, e.g. <http://myCLM.com/clm>.
3. If required, enter your user credentials to log on to the CLM Web site.
4. Click **Request a permanent smart card**.

If you visit the site the first time, an ActiveX control is downloaded and installed.

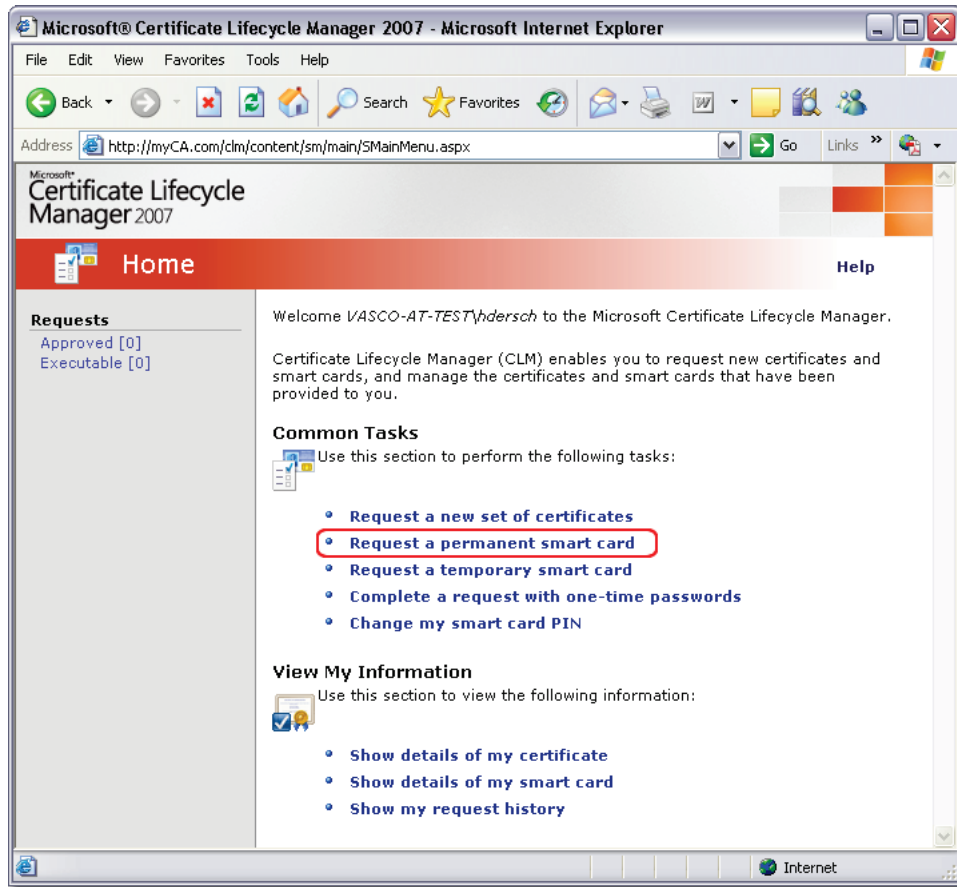


Figure 7: Enrolling a Certificate from Microsoft Certificate Lifecycle Manager (1)

5. Select a profile template in the **Profile Template** list.

The certificate requests are generated and submitted to the certification authority.

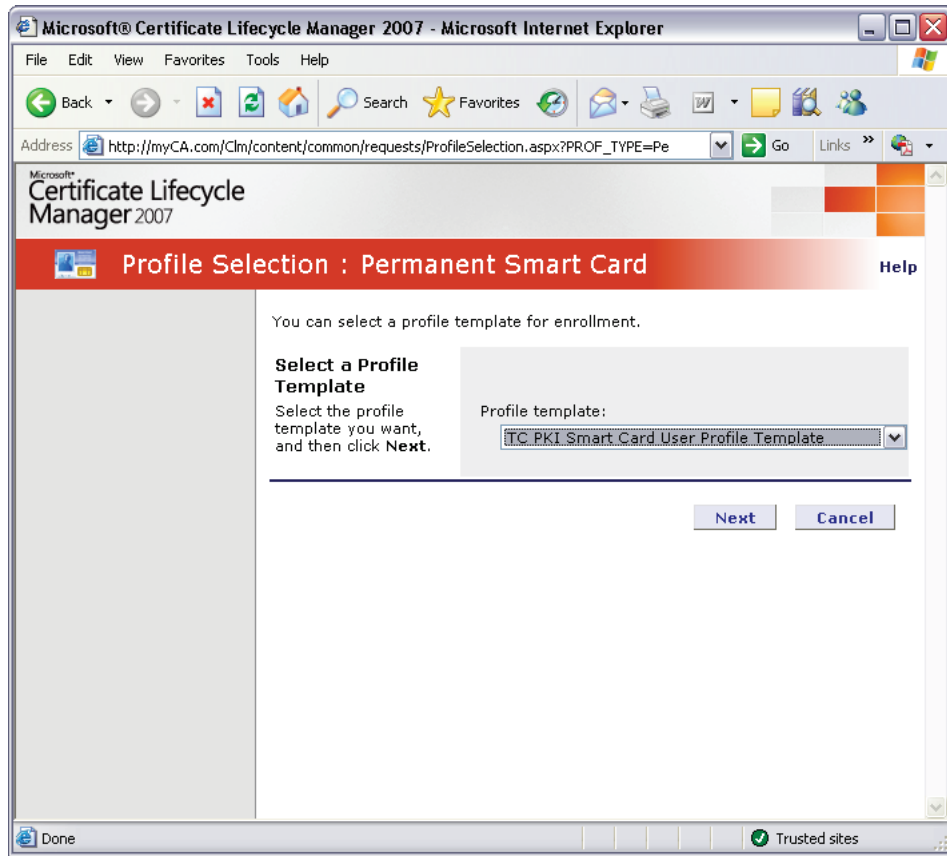


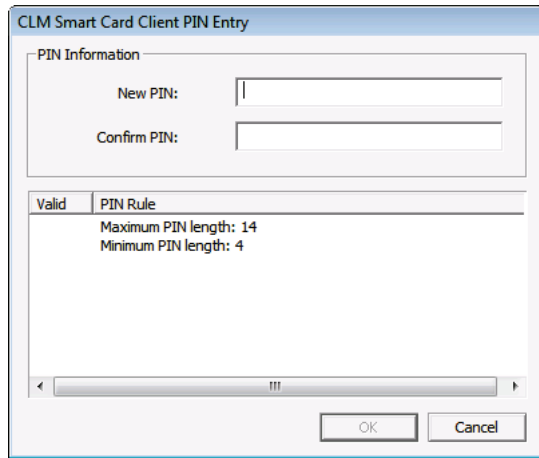
Figure 8: Enrolling a Certificate from Microsoft Certificate Lifecycle Manager (2)

NOTE

If you have access to only one type of profile, CLM does not display the profile selection page.

6. Specify a value for the PIN.

The CLM Client uses the administrator key to set the default PIN to the specified value. The key pairs and certificate requests are finally generated.



The image shows a Windows-style dialog box titled "CLM Smart Card Client PIN Entry". It contains a "PIN Information" section with two text input fields: "New PIN:" and "Confirm PIN:". Below these is a table with two columns: "Valid" and "PIN Rule". The "Valid" column has a single row with the value "True". The "PIN Rule" column contains the text "Maximum PIN length: 14" and "Minimum PIN length: 4". At the bottom of the dialog are "OK" and "Cancel" buttons.

Valid	PIN Rule
True	Maximum PIN length: 14 Minimum PIN length: 4

Figure 9: Enrolling a Certificate from Microsoft Certificate Lifecycle Manager (3)

2.3.3 Additional considerations

- When requesting and enrolling a certificate while two or more valid tokens are connected, the first enumerated token is automatically selected.
- Usually you are required to supersede and configure certificate templates to enroll from existing certificate templates pre-configured on the Microsoft CA.

2.3.4 Additional references

- [Enrolling Certificates from a Microsoft Certification Authority \(CA\) using the CA Web interface](#)
- [Enrolling Certificates from an Entrust Certification Authority \(CA\)](#)

2.4 Enrolling Certificates from an Entrust Certification Authority (CA)

2.4.1 Before you begin

To request and enroll a certificate from an Entrust CA you need:


- the user properly configured in Entrust Authority Security Manager
- a reference number and authorization code for the user account you want to enroll a certificate for
- access to the respective CA
- an initialized token
- **Entrust Intelligence Security Provider (ESP) for Windows 8.x** and **VASCO CertiID Smart Card Crypto Provider** installed

-OR-

Entrust Desktop Solutions 7.x and **DP CertiID PKCS#11 Library** installed

2.4.2 Enrolling a certificate from an Entrust Certification Authority (CA)

➤ To enroll a certificate from an Entrust CA using Entrust ESP for Windows

1. Insert your token.
2. Select **Enroll for Entrust Digital ID** from the Entrust ESP notification area icon menu .

The **Enroll for Entrust Digital ID Wizard** appears.



Figure 10: Enrolling a Certificate from an Entrust CA using Entrust ESP (1)

3. Click **Next** to begin.
4. Enter the reference number and authorization code provided by your administrator.

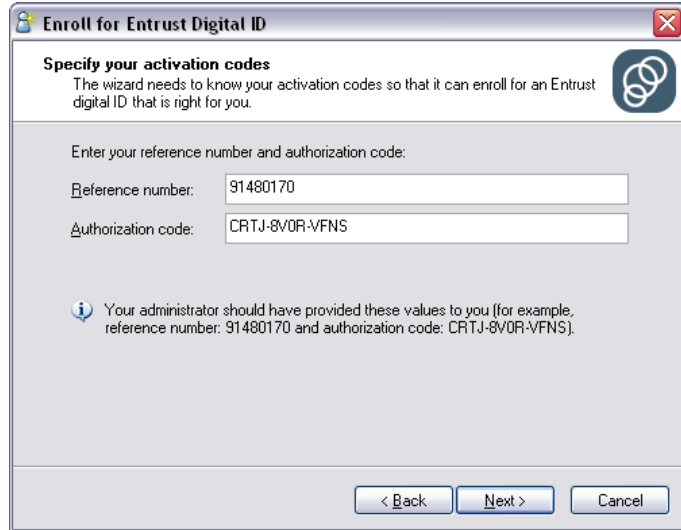


Figure 11: Enrolling a Certificate from an Entrust CA using Entrust ESP (2)

- Click **Next** to start the enrollment.

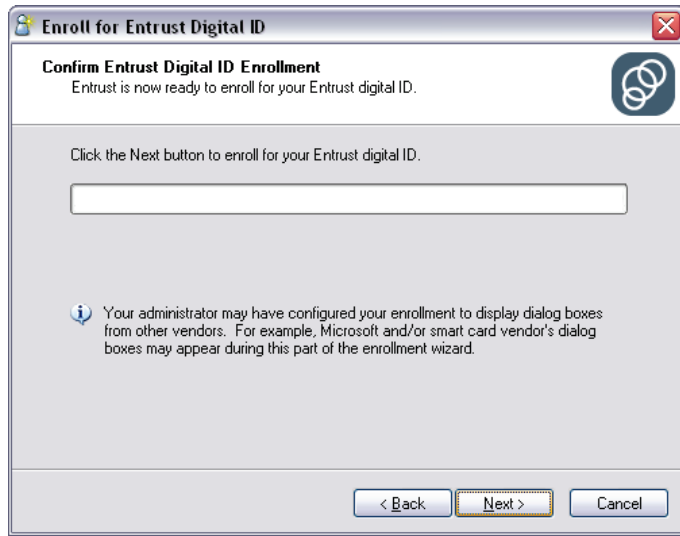


Figure 12: Enrolling a Certificate from an Entrust CA using Entrust ESP (3)

- If required, enter your PIN.
- Click **Finish** to close the wizard.

➤ **To enroll a certificate from an Entrust CA using Entrust Desktop Solutions**

- Insert your token.
- Select **Create Entrust Profile** from the Entrust Desktop Solutions notification area icon menu .

The **Create Entrust Profile Wizard** appears.

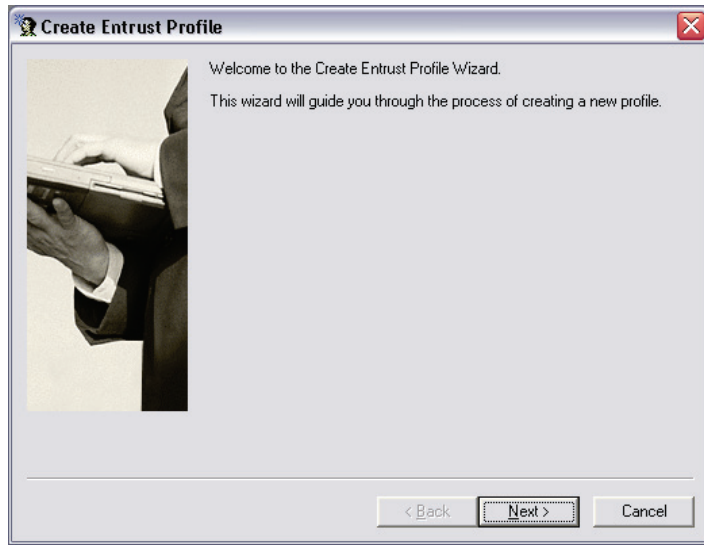


Figure 13: Enrolling a Certificate from an Entrust CA using Entrust Desktop Solutions (1)

3. Click **Next** to begin.
4. Enter the reference number and authorization code provided by your administrator.



Figure 14: Enrolling a Certificate from an Entrust CA using Entrust Desktop Solutions (2)

5. Enable **Store profile on hardware token (card)** and select the token to enroll the certificate on in the list box below.



Figure 15: Enrolling a Certificate from an Entrust CA using Entrust Desktop Solutions (3)

6. Type a name for your profile.



Figure 16: Enrolling a Certificate from an Entrust CA using Entrust Desktop Solutions (4)

- Click **Next** to start the enrollment.



Figure 17: Enrolling a Certificate from an Entrust CA using Entrust Desktop Solutions (5)

- If required, enter your PIN.

NOTE

Entrust Desktop Solutions refers to the PIN as token password.

- Click **Finish** to close the wizard.

2.4.3 Additional considerations

- The new private key associated with the requested certificate is protected by the default PIN, if one is available on the token. You can change this via **DP CertiID Management Application**.

2.4.4 Additional references

- [Enrolling Certificates from a Microsoft Certification Authority \(CA\) using the CA Web](#) interface
- [Enrolling Certificates from Microsoft Certificate Lifecycle Manager](#) (CLM)

3 Signing and Encrypting E-mails

This chapter gives an overview of how to sign or verify signed E-mails and to encrypt or decrypt encrypted E-mails, respectively, with common mail programs using your token and DIGIPASS CertiID.

It covers the following topics:

- Signing and Encrypting E-mails with Microsoft Outlook 2003
- Signing and Encrypting E-mails with Mozilla Thunderbird 2.x

3.1 Signing and Encrypting E-mails with Microsoft Outlook 2003

3.1.1 Before you begin

To sign an E-mail with Microsoft Outlook 2003 you need:

- an initialized token with a valid personal certificate with enhanced key usage for [E-Mail Protection](#)
- either **VASCO CertiID Smart Card Crypto Provider** or **VASCO Card Module** installed and registered as default cryptographic provider
- Microsoft Outlook 2003 configured for E-mail security

Additionally, to encrypt an E-mail with Microsoft Outlook 2003 you need:

- a valid certificate of the recipient you want to send the E-mail

➤ To configure E-mail security in Microsoft Outlook 2003

1. Start Outlook.
2. Select **Tools > Options** from the Outlook menu bar.

The Outlook **Options Dialog** appears.

3. Switch to the **Security** tab.

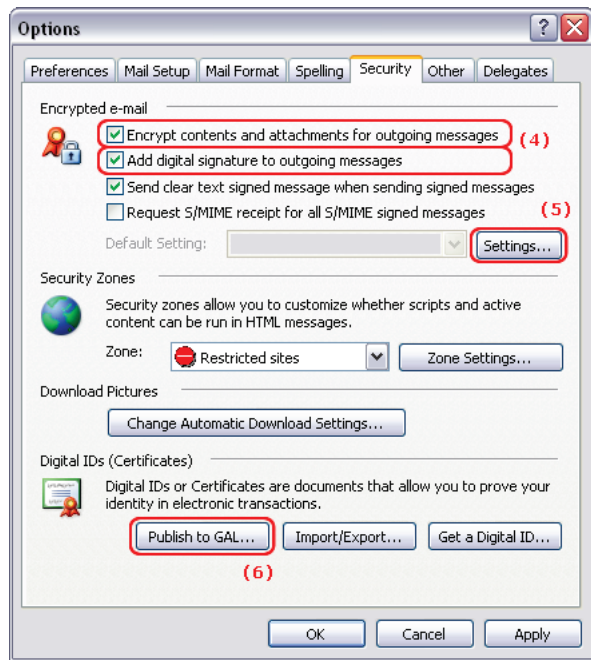


Figure 18: Configuring E-mail security in Microsoft Outlook 2003 (1)

4. Enable **Encrypt contents and attachments for outgoing messages** and **Add digital signatures to outgoing messages**.

- Click **Settings** to create a new settings profile.

The **Change Security Settings Dialog** appears.



Figure 19: Configuring E-mail Security in Microsoft Outlook 2003 (2)


- Type a name for the profile in the **Security Settings Name** box.
 - Select your personal certificate via **Choose** under **Certificates and Algorithms**.
 - Click **OK** to close the **Change Security Settings Dialog** and return to the **Options Dialog**.
- Click **Publish to GAL** to make your certificate available for others.

This step is necessary so that other mail participants can verify your digital signatures and send you encrypted messages.

- Click **OK**.

3.1.2 Signing and Encrypting an E-mail with Microsoft Outlook 2003

➤ To sign and encrypt an E-mail with Microsoft Outlook 2003

- Insert your token.
- Start Outlook.
- Create a new mail without sending it yet.
- Click **Sign Mail**  to sign the E-mail.

5. Click **Encrypt Mail**  to encrypt the E-mail.

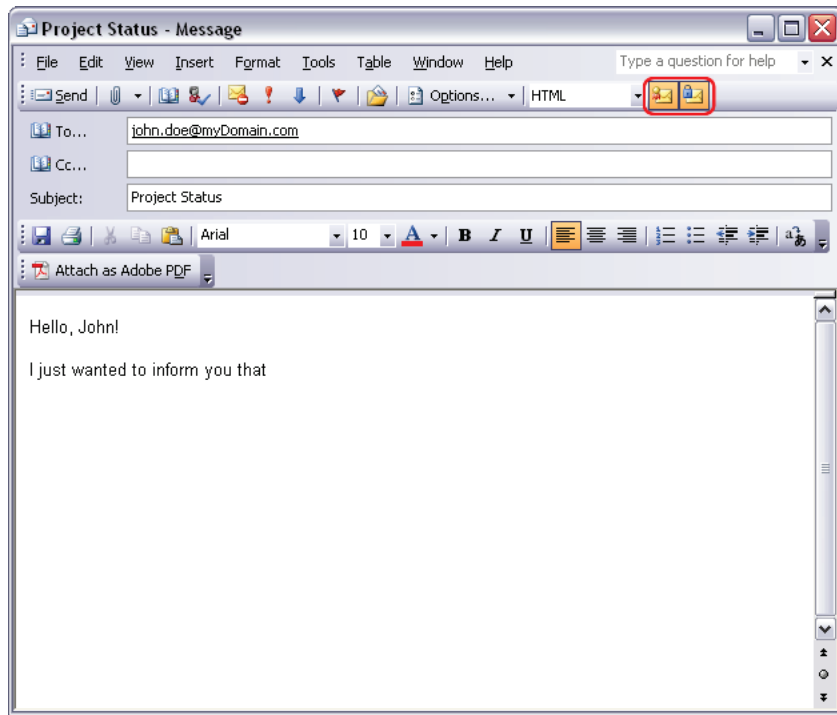



Figure 20: Signing and Encrypting an E-mail with Microsoft Outlook 2003

6. Click **Send**.
7. If required, enter your PIN.

➤ **To decrypt and verify an E-mail with Microsoft Outlook 2003**

1. Insert your token.
2. Start Outlook.
3. Open the encrypted and/or signed E-mail.
4. If required, enter your PIN.

If the mail has been encrypted by the sender, it is automatically decrypted using VASCO CertiID Smart Card Crypto Provider.

5. To verify the authenticity of the E-mail, click the sign icon .

3.1.3 Additional considerations

- You can verify whether the certificate supports E-mail protection by inspecting the certificate's enhanced key usage parameters using **DP CertiID Management Application**.

3.1.4 Additional references

- [Signing and Encrypting E-mails with Mozilla Thunderbird 2.x](#)

3.2 Signing and Encrypting E-mails with Mozilla Thunderbird 2.x

3.2.1 Before you begin

To sign an E-mail with Mozilla Thunderbird 2.x you need:

- an initialized token with a valid personal certificate with enhanced key usage for [E-Mail Protection](#)
- **DP CertiID PKCS#11 Library** installed and registered in Mozilla Thunderbird 2.x
- Mozilla Thunderbird 2.x configured for E-mail security

Additionally, to encrypt an E-mail with Mozilla Thunderbird 2.x you need:

- a valid certificate of the recipient you want to send the E-mail

➤ To register DP CertiID PKCS#11 Library in Mozilla Thunderbird 2.x

1. Start Thunderbird.
2. Do one of the following:
 - If you have selected the [Firefox/Thunderbird Configuration](#) feature when installing DIGIPASS CertiID:
 - Select Tools > Register VASCO DP CertiID PKCS#11 from the Thunderbird menu bar.
 - If you haven't selected the [Firefox/Thunderbird Configuration](#) feature when installing DIGIPASS CertiID:
 - (a) Select **Tools > Options** from the Thunderbird menu bar.

The **Options Dialog** appears.

- (b) Switch to the **Advanced > Certificates** tab.

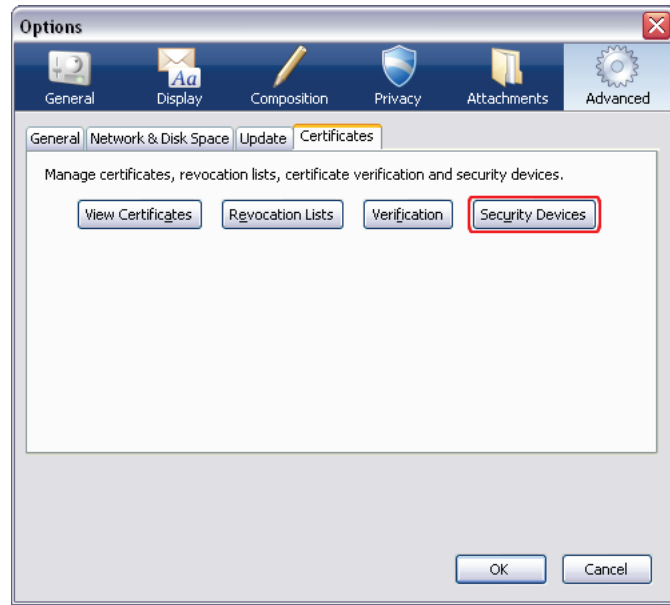


Figure 21: Registering DP CertiID PKCS#11 Library with Mozilla Thunderbird 2.x (1)

- (c) Click **Security Devices**.

The **Device Manager Dialog** appears.

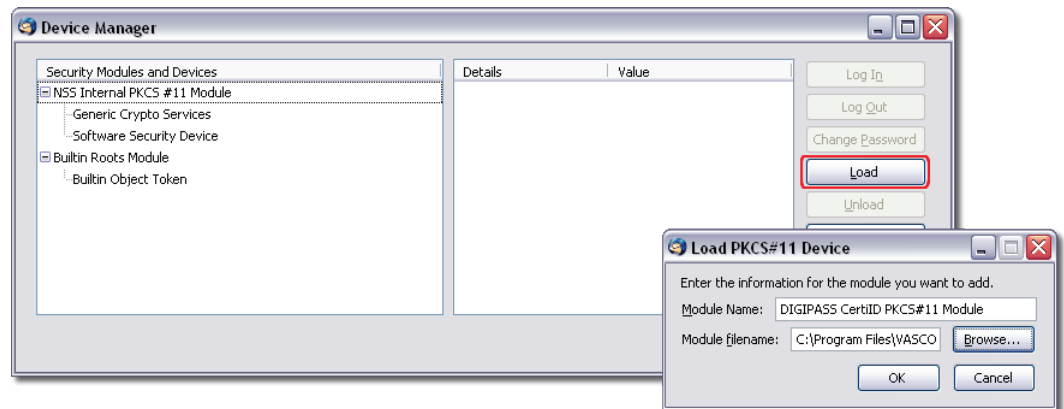


Figure 22: Registering DP CertiID PKCS#11 Library with Mozilla Thunderbird 2.x (2)

- (d) Click **Load**.
- (e) Specify a module name and the module filename of the **DP CertiID PKCS#11 Library**.

In a default installation, this is `C:\Program Files\VASCO\DIGIPASS CertiID\VdsPKCS1132.dll`.

3. Click **OK** to confirm installing the PKCS#11 module.

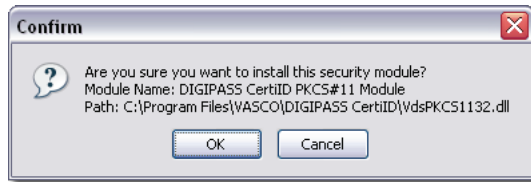


Figure 23: Registering DP CertiID PKCS#11 Library with Mozilla Thunderbird 2.x (3)

➤ To configure E-mail security in Mozilla Thunderbird 2.x

1. Start Thunderbird.
2. Select **Tools > Account Settings** from the Thunderbird menu bar.

The **Account Settings Dialog** appears.

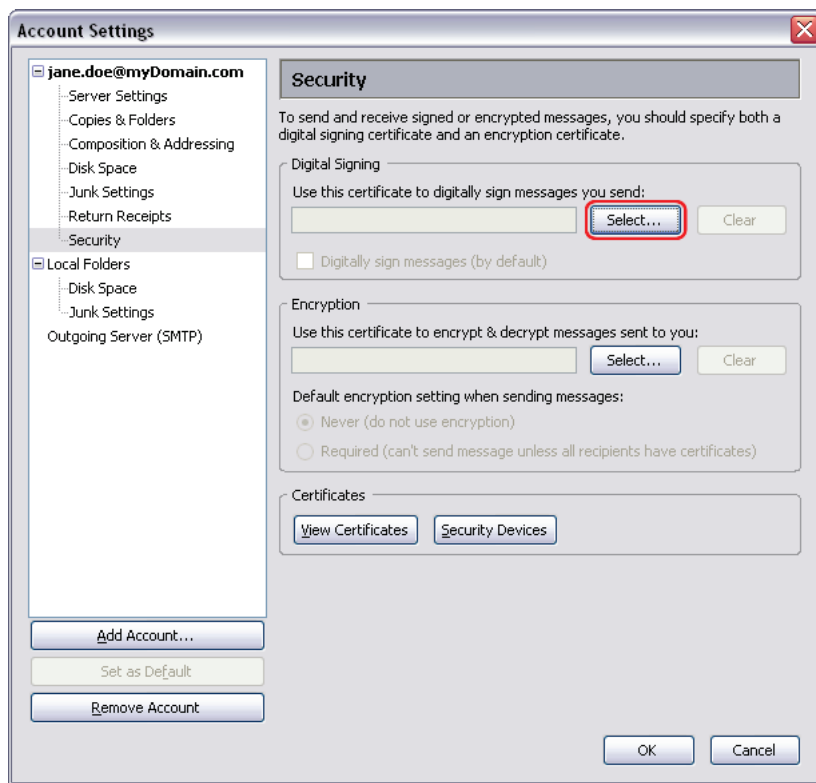


Figure 24: Configuring E-mail Security in Mozilla Thunderbird 2.x

3. Expand the item for your respective E-mail account and select **Security**.
4. Click **Select** to select a certificate used to digitally sign E-mails.

5. If required, enter your PIN.

NOTE

Mozilla Thunderbird refers to the PIN as master password.

6. Select a certificate to use to digitally sign and/or encrypt E-mails.
7. Click **OK**.

3.2.2 Signing and Encrypting an E-mail with Mozilla Thunderbird 2.x

- To sign and encrypt an E-mail with Mozilla Thunderbird 2.x
1. Insert your token.
 2. Start Thunderbird.
 3. Create a new E-mail without sending it yet.
 4. Select **Security > Encrypt This Message** in the Thunderbird toolbar to sign the E-mail.
 5. Select **Security > Digitally Sign This Message** in the Thunderbird toolbar to sign the E-mail.

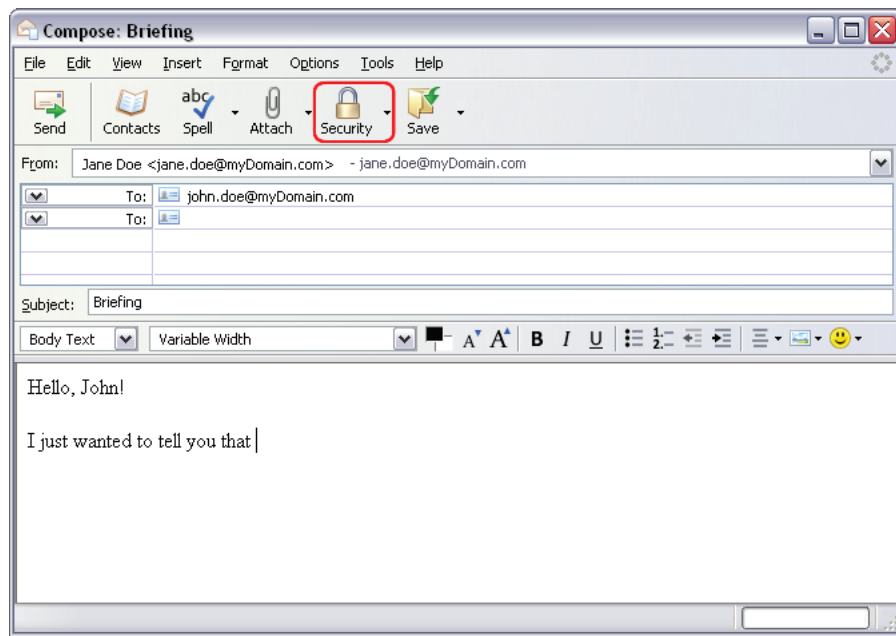


Figure 25: Signing and Encrypting an E-mail with Mozilla Thunderbird 2.x

6. Click **Send**.
7. If required, enter your PIN.

3.2.3 Additional considerations

- You can verify whether the certificate supports E-mail protection by inspecting the certificate's enhanced key usage parameters using **DP CertiID Management Application**.
- It is not recommended to use different PINs (other than the default PIN) with PKCS #11, since some PKCS #11 applications do not support context-specific authentication, including Mozilla Thunderbird 2.x.

3.2.4 Additional references

- [Signing and Encrypting E-mails with Microsoft Outlook 2003](#)

4 Signing Documents

This chapter gives an overview of how to sign or verify signed documents with common applications using your token and DIGIPASS CertiID.

It covers the following topics:

- Signing Documents with Adobe Acrobat 8.x

4.1 Signing Documents with Adobe Acrobat 8.x

4.1.1 Before you begin

To sign a document with Adobe Acrobat 8.x you need:

- an initialized token with a valid personal certificate
- either **VASCO CertiID Smart Card Crypto Provider**, **VASCO Card Module**, or **DP CertiID PKCS#11 Library** installed

4.1.2 Signing a document with Adobe Acrobat 8.x

- To sign a document with Adobe Acrobat 8.x
1. Insert your token.
 2. Start Acrobat.
 3. Create or open a document to sign.
 4. Select **Advanced > Sign & Certify > Place Signature** from the Acrobat menu bar.

5. Click and drag in the document to draw a signature field where you would like the signature to appear.

The **Sign Document Dialog** appears.

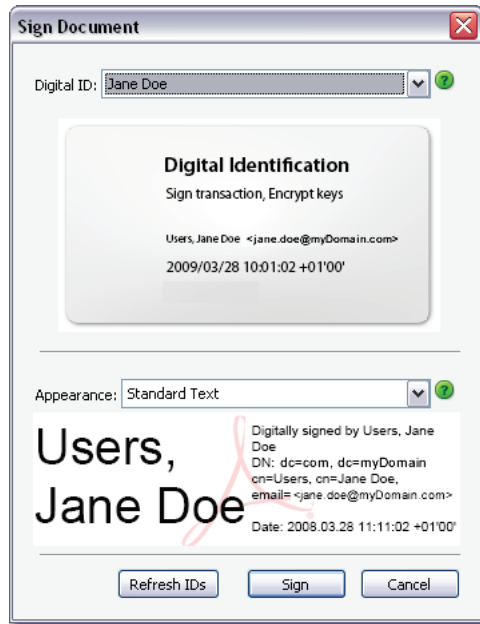


Figure 26: Signing a Document with Adobe Acrobat 8.x

6. Select your certificate in the **Digital ID** list and click **Sign**.

The **Save As Dialog** appears.

7. Specify a new file name to save the signed document.
8. If required, enter your PIN.

4.1.3 Additional considerations

- If the document does not contain a signature, you can also add a certifying signature (via **Advanced > Sign & Certify > Sign Document**), which allows you to restrict changes to the document.

4.1.4 Additional references

- [Encrypting Documents with Adobe Acrobat 8.x](#)

5 Encrypting Documents

This chapter gives an overview of how to encrypt documents with common applications using your token and DIGIPASS CertiID.

It covers the following topics:

- Encrypting Documents with Adobe Acrobat 8.x

5.1 Encrypting Documents with Adobe Acrobat 8.x

5.1.1 Before you begin

To encrypt a document with Adobe Acrobat 8.x you need:

- an initialized token with a valid personal certificate
- either **VASCO CertiID Smart Card Crypto Provider**, **VASCO Card Module**, or **DP CertiID PKCS#11 Library** installed
- Adobe Acrobat 8.x configured for signing

5.1.2 Encrypting a document with Adobe Acrobat 8.x

➤ To encrypt a document with Adobe Acrobat 8.x

1. Insert your token.
2. Start Acrobat.
3. Create or open a document to encrypt.

NOTE

You can't encrypt a signed or certified document.

4. Select **Advanced > Security > Certificate Encrypt** from the Acrobat menu bar.

The **Certificate Security Settings Dialog** appears.

5. Set encryption settings in the **General settings** tab.
6. Select the recipients who are supposed to be able to open the document in the **Select recipients** tab.
7. Click **Finish**.
8. Save the document.

5.1.3 Additional references

- [Signing Documents with Adobe Acrobat 8.x](#)

6 Encrypting Files and Folders

This chapter gives an overview of how to use your token and DIGIPASS CertiID to encrypt and decrypt files and folders via Encrypting File System (EFS).

It covers the following topics:

- Encrypting and Decrypting Files and Folders via Encrypting File System (EFS)
- Recovering Data for Encrypting File System (EFS)

6.1 Encrypting and Decrypting Files and Folders via Encrypting File System (EFS)

The Encrypting File System (EFS) allows you to protect confidential data by encrypting files or folders on NTFS. You can use digital certificates for EFS to secure access to the encrypted files and folders.

6.1.1 Before you begin

To encrypt a file or a folder with Encrypting File System (EFS) you need:

- an initialized token containing a valid personal certificate with enhanced key usage for [Encrypting File System](#)
- **VASCO Card Module** installed and registered as default cryptographic provider
- a client machine (with Microsoft Windows Vista SP 1 or higher) joined to a Windows domain (Microsoft Windows Server 2008) and with access to a configured certification authority (CA)
- a hard disk or volume using NTFS
- Domain Group Policy enabling Encrypting File System
- Domain Group Policy configuring Encrypting File System to require smart card

TIP

When you create a certificate template to enroll certificates for Encrypting File System, you should consider selecting **Archive subject's encryption private key** in the **Request Handling** tab to enable key archiving for key recovery.

➤ To enable and configure Encrypting File System via Group Policy (Windows Server 2008)

1. Start **Group Policy Management** via command prompt by typing `gpmc.msc`.
2. Select the Group Policy object in the Group Policy management tree, e.g. [Default Domain Policy](#).
3. Select **Edit** from the context menu.

The **Group Policy Management Editor** appears.

4. Select **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies > Encrypting File System** in the Group Policy Object tree.
5. Select **Properties** from the context menu.

The **Encrypting File System Properties Dialog** appears.

6. Select **Allow** to enable EFS.
7. Select **Require a smart card for EFS**.

8. Clear **Allow EFS to generate self-signed certificates when a certification authority is not available** to restrict EFS to tokens.
9. Click **OK** to close the **Encrypting File System Properties Dialog**.
10. Close **Group Policy Object Editor**.

NOTE

You should consider which data recovery method you want to use, before you begin using Encrypting File System (EFS).

6.1.2 Encrypting a file or a folder using Encrypting File System (EFS)

**To encrypt a file or a folder**

1. Insert your token.
2. Select the respective file or folder you want to encrypt.
3. Select **Properties** from the context menu.
4. Switch to the **General** tab and click **Advanced**.

The **Advanced Attributes Dialog** appears.

5. Select **Encrypt contents to secure data** and click **OK**.
6. Click **OK** to close the **Properties Dialog**.
7. Select what you want to encrypt.
 - If you are encrypting a file, you are prompted whether to encrypt the file only or the parent folder containing the file.
 - If you are encrypting a folder, you are prompted whether to encrypt that folder only or the folder including all subfolders and files.
8. If required, select the certificate to use for file encryption.

This step is only necessary the first time you encrypt a file or a folder using a new certificate.

9. If required, type your PIN.

The selected files and/or folders is/are encrypted. Encrypted files and folders are indicated by a different label color, by default green.

NOTE

You need to type the PIN the first time you try to use EFS in a session. If you are not prompted to type a PIN, look in the notification area for the **Encrypting File System** icon and click it to bring the **Windows Security Dialog** to the desktop.

NOTE

The PIN is being cached for subsequent encryption until you log off.

➤ To open an file protected using Encrypting File System

1. Insert your token.
2. Open the file.
3. If required, type your PIN.

The encrypted file is decrypted and opened.

NOTE

You need to type the PIN the first time you try to use EFS in a session. If you are not prompted to type a PIN, look in the notification area for the **Encrypting File System** icon and click it to bring the **Windows Security Dialog** to the desktop.

6.1.3 Decrypting a file or a folder using Encrypting File System (EFS)

Decrypting a file or a folder means to remove the encryption protection.

➤ To decrypt a file or a folder

1. Insert your token.
2. Select the respective file or folder.
3. Select **Properties** from the context menu.
4. Type your PIN.
5. Switch to the **General** tab and click **Advanced**.

The **Advanced Attributes Dialog** appears.

6. Clear **Encrypt contents to secure data** and click **OK**.
7. Select what you want to decrypt.
8. Click **Apply**.

6.1.4 Additional considerations

- If you encrypt a folder, any file that you create in that folder will be automatically encrypted as well.
- If you copy or move a file to a disk that does not use NTFS, the file will be decrypted.

- You can verify whether the certificate supports smart card logon by inspecting the certificate's enhanced key usage parameters using **DP CertiID Management Application**.

6.1.5 Additional references

- [Requesting and Enrolling Certificates](#)
- [Recovering Data for Encrypting File System \(EFS\)](#)

6.2 Recovering Data for Encrypting File System (EFS)

Recovering data encrypted using Encrypting File System (EFS) can be achieved by two different methods:

- **File recovery**

File recovery means that an encrypted file or folder is decrypted using an file recovery agent certificate.

This method is applicable for instance, if the token with the user certificate and private key used to encrypt the file is damaged and the private key cannot be retrieved from the certification authority (CA).

It implies that someone other than the owner may access the encrypted data of the owner!

- **Key recovery**

Key recovery means to retrieve a copy of the private key used to encrypt the file from the certification authority (CA) database.

This method is applicable, if the token with the user certificate and private key used to encrypt the data is damaged.

It implies that someone other than the owner may access the private key of the owner!

TIP

You can use either file recovery or key recovery, or both, respectively.

This section gives a brief overview about these two methods. For detailed information and throughout discussion, refer to corresponding Microsoft resources.

6.2.1 Before you begin

NOTE

You should consider which data recovery method you want to use and prepare it, BEFORE you begin using Encrypting File System (EFS).

You cannot recover data that had been encrypted before the respective recovery method was prepared.

To recover data for Encrypting File System (EFS) using file recovery you need:

- to configure a data recovery agent, i.e. a user with a published and valid certificate with enhanced key usage for [Data Recovery Agent](#)

CAUTION

Use file recovery, if you require the ability to recover data, but don't want anyone else other than the respective owner to access the individual private keys.

➤ To configure a data recovery agent

1. Start **Group Policy Management** via command prompt by typing `gpmmc.msc`.
2. Select the Group Policy object in the Group Policy management tree, e.g. [Default Domain Policy](#).
3. Select **Edit** from the context menu.

The **Group Policy Management Editor** appears.

4. Select **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies > Encrypting File System** in the Group Policy Object tree.
5. Select **Add Data Recovery Agent** from the context menu.

The **Add Data Recovery Agent Wizard** appears.

6. Configure the data recovery agent by following the instructions in the **Add Data Recovery Agent Wizard**.

To recover data for Encrypting File System (EFS) using key recovery you need:

- enable key archiving on the certification authority (CA)
- a valid key recovery agent certificate, i.e. a valid certificate with enhanced key usage for [Key Recovery Agent](#)
- the serial number of the certificate to be recovered

CAUTION

Key archiving is a very sensible and powerful feature, since it allows a certification authority (CA) administrator to decrypt any data that utilizes a private key signed by the CA.

Treat key archiving and recovery very carefully!

6.2.2 Recovering data for Encrypting File System (EFS) using file recovery

➤ To recover encrypted data using file recovery

1. Insert your token with the file recovery agent certificate.
2. Select the respective file or folder.
3. Select **Properties** from the context menu.
4. Type your PIN.
5. Switch to the **General** tab and click **Advanced**.

The **Advanced Attributes Dialog** appears.

6. Clear **Encrypt contents to secure data** and click **OK**.
7. Select what you want to decrypt.
8. Click **Apply**.

The files and/or folders are decrypted using the file recovery agent key.

TIP

You can inspect which recovery certificates are defined via **Details** in the **Advanced Attributes Dialog** of the respective file or folder.

6.2.3 Recovering data for Encrypting File System (EFS) using key recovery

➤ **To recover encrypted data using key recovery (conceptional overview)**

1. Retrieve a PKCS #7 BLOB from the certification authority (CA) database (using [certutil.exe](#)).

The PKCS #7 BLOB contains the certificate and the encrypted private key to be recovered. The private key information is encrypted using the key recovery agent public key.

2. Decrypt the private key stored in the BLOB using the key recovery agent certificate (using [certutil.exe](#)).

This creates a protected PKCS #12 file that can be delivered to the user.

3. Import the recovered PKCS #12 file.

6.2.4 Additional references

- [Requesting and Enrolling Certificates](#)

7 Certificate-based Authentication

This chapter gives an overview of how to use your token and DIGIPASS CertiID for certificate-based authentication to common operating systems or applications.

It covers the following topics:

- Authenticating to Microsoft Windows XP/2000
- Authenticating to Microsoft Windows Vista

7.1 Authenticating to Microsoft Windows XP/2000

7.1.1 Before you begin

To authenticate to Microsoft Windows XP/2000 using a certificate you need:

- an initialized token containing a valid personal certificate with enhanced key usage for [Smart Card Logon](#)
- **VASCO CertiID Smart Card Crypto Provider** installed
- Microsoft Windows configured for certificate-based authentication
- a client machine joined to a Windows domain and with access to a configured certification authority (CA)

7.1.2 Authenticating to Microsoft Windows XP/2000

➤ To authenticate to Microsoft Windows XP/2000 using a certificate

1. Insert your token at the **Windows Welcome Dialog**.
2. If required, enter your PIN.

Microsoft Windows uses the default container to authenticate and logs you on.

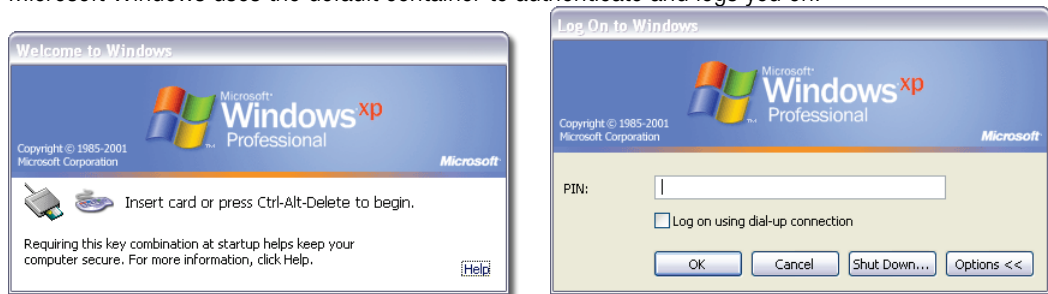


Figure 27: Authenticating to Microsoft Windows XP/2000 using a Certificate

7.1.3 Additional considerations

- You can verify whether the certificate supports smart card logon by inspecting the certificate's enhanced key usage parameters using **DP CertiID Management Application**.
- The default certificate container is used for authentication. If you have more than one certificate containers on your token, you need to explicitly set a default container using **DP CertiID Management Application**.

- Due to the nature of Microsoft Windows CSP handling, you will not get an appropriate error message when the PIN is blocked, but that a wrong PIN has been entered.
- If you remove the token after login, the card remove action defined by domain security policies is executed.

7.1.4 Additional references

- [Authenticating to Microsoft Windows Vista](#)

7.2 Authenticating to Microsoft Windows Vista

7.2.1 Before you begin

To authenticate to Microsoft Windows Vista using a certificate you need:

- an initialized token containing a valid personal certificate with extended key usage for [Smart Card Logon](#)
- either **VASCO CertiID Smart Card Crypto Provider** or **VASCO Card Module** installed
- Microsoft Windows configured for certificate-based authentication
- A client machine joined to a Windows domain and access to a configured certification authority (CA)

7.2.2 Authenticating to Microsoft Windows Vista

➤ To authenticate to Microsoft Windows Vista using a certificate

1. If required, press CTRL-ALT-DELETE at the **Windows Welcome Dialog**.
2. Insert your token at the **Select User Screen**.

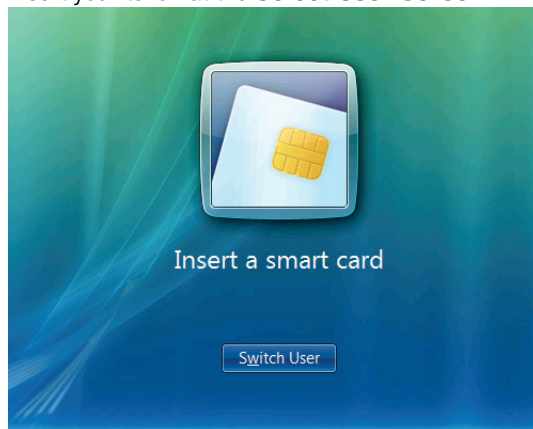


Figure 28: Authenticating to Microsoft Windows Vista using a Certificate

3. If required, select the certificate you want to use for authentication.

If more than one certificate container exists on the token, the available user accounts are shown at the **Select User Screen**.

4. If required, enter your PIN.

Microsoft Windows uses the selected certificate container to authenticate and logs you on.

7.2.3 Additional considerations

- You can verify whether the certificate supports smart card logon by inspecting the certificate's enhanced key usage parameters using **DP CertiID Management Application**.
- If you are using **VASCO Card Module** you cannot use keypad reader hardware to authenticate under Microsoft Windows Vista, but are required to type the PIN via the screen dialog.
- If you remove the token after login, the card remove action defined by domain security policies is executed.

7.2.4 Additional references

- [Authenticating to Microsoft Windows XP/2000](#)

Index

- A**
- administrator key 20
 - Adobe Acrobat
 - encrypting documents 45
 - signing documents 42
- C**
- CA *See* Certification Authority (CA)
 - card module 11, 13, 15, 20, 31, 42, 45, 47, 57
 - card remove action 56, 58
 - certificate
 - enrolling 10
 - enrolling, from Entrust CA 10, 14, 24
 - enrolling, from Microsoft CA 11, 15
 - enrolling, from Microsoft Certificate Lifecycle Manager (CLM) 20
 - enrolling, using Entrust Desktop Solutions 26
 - enrolling, using Entrust Entelligence Security Provider (ESP) 24
 - certificate container 55
 - Certification Authority (CA)
 - requesting certificates 10
 - CLM *See* Microsoft Certificate Lifecycle Manager (CLM)
 - Cryptographic Service Provider (CSP) 11, 13, 15, 24, 31, 34, 42, 45, 55, 57
- D**
- document conventions 8
 - documents
 - encrypting 44
 - encrypting, using Adobe Acrobat 8 45
 - signing 41
 - signing, using Adobe Acrobat 8 42
- E**
- EFS *See* Encrypting File System (EFS)
 - E-mail
 - decrypting, using Microsoft Outlook 2003 34
 - encrypting 30
 - encrypting, using Microsoft Outlook 2003 31, 33
 - encrypting, using Mozilla Thunderbird 2.x 36, 39
 - signing 30
 - signing, using Microsoft Outlook 2003 31, 33
 - signing, using Mozilla Thunderbird 2.x 36, 39
 - verifying, using Microsoft Outlook 2003 34
 - E-mail security
 - configuring Microsoft Outlook 2003 31
 - configuring Mozilla Thunderbird 2.x 38
 - Encrypting File System (EFS)
 - data recovery agent 52
 - decrypting files 49
 - encrypting files 47
 - key recovery agent 52
 - recovering data using file recovery 52
 - recovering data using file recovery, Caution notice 51
 - recovering data using key recovery 53
 - recovering data using key recovery, Caution notice 52
 - recovering files 51
 - Entrust Certification Authority (CA)
 - requesting certificates 24
- F**
- file recovery, Caution notice 51
 - files, encrypting using Encrypting File System (EFS) 47
- K**
- key recovery, Caution notice 52
 - key set
 - creating 13
 - using existing set 13
- M**
- Microsoft Certificate Lifecycle Manager (CLM) 20
 - profile template 20
 - requesting certificates 20
 - requesting certificates, using CLM Web interface 20
 - Microsoft Certification Authority (CA)
 - requesting certificates using Microsoft Management Console (MMC) 15
 - requesting certificates, using CA Web interface 11, 12
 - requesting certificates, using Microsoft Management Console (MMC) 15
 - Microsoft Outlook
 - configuring E-mail security 31
 - decrypting E-mails 34
 - encrypting E-mails 31, 33
 - signing E-mails 31, 33
 - verifying E-mails 34
 - Microsoft Windows
 - authenticating 55, 57
 - authenticating, card remove action 56, 58
 - minimum key length 14
 - Mozilla Thunderbird 40
 - configuring E-mail security 38
 - encrypting E-mails 36, 39
 - signing E-mails 36, 39

P	
Personal Identification Number (PIN)	
default PIN	14, 29
PIN	<i>See</i> Personal Identification Number (PIN)
PKCS ..	<i>See</i> Public Key Cryptography Standards (PKCS)
private key	14, 29
Public Key Cryptography Standards (PKCS)	
PKCS #11 module	24, 36, 42, 45
Public Key Cryptography Standards (PKCS) #11	
40	
U	
user authentication	
Microsoft Windows Vista	57
Microsoft Windows XP/2000	55
Microsoft Windows XP/2000, card remove action .	56,
58	